EB Docket No: 04-296

Subject: Comments Regarding Equipment and Operational Issues Identified Following the First Nationwide Test of the Emergency Alert System

November 4, 2013

Dear Federal Communications Commission,

I would like to comment on the questions posed by the Public Safety and Homeland Security Bureau and offer some suggestions regarding equipment and operational issues identified following the first nationwide test of the Emergency Alert System.

1. Publish a List of Objectives and Expectations for National EAS Operation (Concept of Operations)

Parts of the first nationwide test of the Emergency Alert System performed well. Because there are ambiguities in every technical protocol standard, and different implementers resolve those ambiguities in different ways, a well-documented list of objectives is important to guide interoperability between various implementations and alerting standards which interconnect with EAS.

Attempting to infer objectives and expectations from technical protocol specification is like reading tea leaves. Technical protocol specifications tend to reflect whatever technology was used at the time, including limitations of that technology.

Beginning in 1951 with CONELRAD, in 1960's with Emergency Broadcast System and 1990's with Emergency Alert System, a national plan and statement of requirements was published which helped guide the development of technical operations and protocols to achieve those objectives. Those planning documents were published by other stakeholders such as Civil Defense Agency, Federal Emergency Management Agency and advisory commissions while the FCC published implementing rules. Although there is no longer a publically published National EAS Plan or stakeholder list of objectives, the FCC has continued making piecemeal changes to the audible-digital EAS protocol rules in 47 C.F.R. Part 11. Without a published list of objectives for a national alert plan, it is difficult to determine if a particular change would improve implementation or operation.

For example, other alerting protocol standards such as ANSI/SCTE 18 2007 "Emergency Alert Messaging for Cable," ATIS-0800010 "Emergency Alert Service Provisioning Specifications," NOAA "NWR Specific Area Message encoding," and CEA-2009-B (ANSI) "Receiver Performance Specification for Public Alert Receivers" inter-operate with the EAS protocol, but each has implementation and operation variations. Those differences may or may not be significant depending on the list of objectives and expectations.

An alternative may be to recognize a standards body to maintain the audible-digital EAS technical protocol standard and publish the concept of operations as part the FCC rules. This could make it easier to maintain related FCC material such as EAS Handbooks and adapt to future technologies.

Because the audio portion of the EAN wasn't handled well, future EAN tests may show differences in audio handling between EAS participants.

1) Join an EAN broadcast feed in progress, or start replay at the beginning after lengthy head-end equipment switching
2) A station receives an EAN overnight while off the air, and returns to the air after the EAN is complete in the morning.
3) Synchronizing feeds or switching to a better network feed during a long EAN

2. EAS Header: Time of Release Code

The WRSAME protocol, which the EAS protocol is based, was written when many weather receivers did not include real-time clocks. WRSAME messages were effective immediately upon issuance and valid until the purge time. Weather receivers without real-time clocks estimate the purge time using only the delta time field "+TTTT" and a simple countdown timer. The NWR SAME protocol document (NWR Specific Area Message Encoding, Update #4.43, July 13, 1999) does not explicitly use the date-time field "-JJJHHMM" in weather receivers. CEA-2009-B, Public Alert compliant receivers do not appear to check the time for duplicate or already expired SAME messages.

EAS decoders have multiple receiver inputs and daisy-chain re-transmission delays requiring more complicated duplicate and expired message processing than simple weather radios. But the principle would be the same: "EAS messages are effective immediately upon issuance and valid until the purge time and not a duplicate message."

A variation of a duplicate EAS message is a replay attack. EAS replay attacks cannot be completely mitigated because the EAS protocol Julian date field "-JJJHHMM" repeats every year. A message with a "future" time may actually be a replay of a very "old" message. Due to its power, EAN messages are likely candidates for forged and replay attacks. EAN messages should meet valid time period checks to minimize those replay time windows. A replay attack may be unintentional. After the National EAS test, several local reporters replayed recordings of the EAN test tones on the air during their news reports.

An additional challenge is real-time clocks in EAS decoders or encoders may be incorrect. While rare, time synchronization services such as GPS, NTP and WWV/WWVB have had clock glitches. Operator error configuring clocks in EAS decoders have also occurred. Requiring highly synchronized clocks between diverse EAS equipment or attempting nationwide synchronized message release through diverse technologies will make all the protocols more brittle to clock problems.

One way to resolve the protocol time and duplicate checks is upon receiving an EAS message, check if the current time is within the EAS message's valid time window from (JJJHHMM minus 60 minutes) until (JJJHHMM+TTTT plus 60 minutes) including the clock skew allowance. This would not delay valid EAS messages with minor clock skew issues, i.e. effective immediately upon issuance, while still protecting against duplicate or replayed messages, i.e. valid until the purge time, unless too long expired or too far in the future. A reasonable range for the clock skew allowance would be between 15 minutes and 90 minutes.

The Common Alerting Protocol (CAP) and NOAA National Weather Wire VTEC include more ways to express times including times of current, future and past events. The EAS-CAP Implementation Group should specify if, when and how to translate those complex times about events into the EAS protocol's simple valid time period.

3. EAS Header: Location Code "000000"

EAN messages require several types of "special" handling. The interaction between EAN, originators and location codes is already complex. A published national EAS plan including a list of objectives would help with what combinations should be supported. Whatever the decision, clarity by the FCC and the expected users of the Location Code use and all types of national messages would help all implementers.

Some of the potential interactions needing resolution for the EAS Header for EAN handling:

1) Originator: Only PEP or could other originators use "national" location?
2) Event code: Only EAN, or could EAT, NPT or NIC or other events use "national" location?
3) Locations: Single "national" location, multiple locations plus "national", no locations?

Adding a national location code, "000000", and reducing the special features of EAN to only unlimited message duration, e.g. normal matching rules for originator code, location code, location translation lookup tables, etc. could simplify new EAS implementations, configurations and translations with other emergency alerting protocols. Adding a national location code, but not clarifying other EAS Header components for an EAN and other national event codes would still have consistency concerns. If a national location code "000000" is not added, would NPT, NIC and EAT also bypass normal location checks?

The EAS header structure should be consistent for all event codes including at least one location code for EAN. Omitting all location codes for an EAN will often require special handling in lower-level decoding and validation code in EAS decoders, meaning more software code paths will not be tested during ordinary EAS messages and tests.

In previous rulemakings, the FCC has added marine location codes and event codes. Daylight savings time rules have changed. NOAA and CEA have included more detailed location code processing in CEA-2009-B, Performance Specification for Public Alert Receivers, section 5.1 Location Code Response including how to handle "000000". Delay adding a national location code "000000" just increases the time it will take to implement a change.

4. National Test Event Code

Regular testing by expected originators at every level (national, state, local, territory, etc.) is necessary. Closed circuit testing can be done frequently to verify equipment and operator readiness. But public tests should be only as frequent to maintain public education.

National originators (PEP) should conduct a scheduled nation-wide public test in odd-number years in November, to avoid national election years, using the National Periodic Test (NPT) event code with the

normal two minute message limit or text to speech via CAP. State/Local originators (CIV/EAS/NWS) could conduct scheduled quarterly or semi-annual public tests using the Required Monthly Test (RMT) event code. Every originator and relay should conduct regular tests (scheduled or random) using the Required Weekly Test (RWT) on communication channels being monitored by other EAS participants. Reducing the reliance on EAS daisy-chain transmissions over the main audio channel of broadcast stations would improve reliability and reduce public fatigue from testing and non-relevant activations. Non-originator and non-relay participants should not be required to originate weekly tests, but may originate RWT/DMO for local equipment testing or on request during an inspection to check if the equipment is working and connected properly.

Due to the special behavior of the EAN event code, it is necessary to have a test code which exactly mimics the EAN except the event code translation. Since EAT is apparently no longer needed, it's translation could be changed to "Emergency Action Test" code with the same behavior as EAN, including immediate override except an EAN, no message limit and nationwide effect. FCC should verify whether EAN-like capability is still needed now that a much larger number of communication networks and technologies are available. If an EAN-like capability is needed, an EAN or revised EAT test code should be tested on a longer cycle due to its public disruption. An EAN or revised EAT test code including a message longer than two minutes should be conducted every 6 to 10 years, replacing the NPT in an odd-numbered year.

Future EAN tests should include other integrated alerting systems, such as Wireless Emergency Alerts for mobile devices, when it is decided how EAN would work over non-EAS protocol systems.

5. Impact of National Test Length on EAS Equipment

Previous Emergency Broadcast System and Emergency Alert System publications emphasized the long, unlimited nature of EAN activations and included two to five minute "talk-up" scripts while circuits were re-configured followed by an EAT at some indeterminate time, possibly days, later. How to optimally insert a brief, 120 second advertisement length message versus a potentially joining a "live" multi-day network feed may vary depending on assumptions.

The best interoperability tests include both the minimum and maximum, valid and invalid, and multiple tests in between. If a full EAS test suite existed, many variations could be tested by implementers and operators instead of relying on the creativity of operators to guess at how various corner-cases should be handled based on FCC handbooks and ambiguities in FCC rules. Due to the lack of an EAN test code, operators often install EAS equipment in non-traditional, complicated head-ends without being able to conduct end-to-end EAN testing due to the fear of accidently triggering a real EAN. Problems may not appear until a "real" EAN occurs.

Establishing regular national tests, even if every 6 to 10 years, would help flush out assumptions about short and long EAN activations.

Thank you for your attention,

Sean Donelan